RGPD
L'important, c'est d'entrer dans la démarche

© FOTOLIA

Le nouveau Règlement européen sur la protection des données personnelles[1] (RGPD), adopté en 2016, entre en vigueur le 25 mai, autant dire demain. Ce RGPD instaure de nouveaux droits pour les individus et de nouvelles obligations pour les structures qui collectent et traitent ces données. Et les sanctions peuvent être importantes. Alors, que faut-il savoir et faire à minima sur le sujet ?

Le règlement européen qui renforce la protection des données personnelles entre donc en vigueur le 25 mai 2018. En posant le premier cadre de protection transnationale des données personnelles, l'Europe est pionnière en la matière. En résumé, la collecte et le traitement des données personnelles dites sensibles restent interdits sauf exceptions. Les données de santé font bien entendu partie des données identifiées comme sensibles.

L'essentiel sur le RGPD

Qui est concerné ? Toutes les structures de santé, sans exception, sont concernées par ce nouveau règlement. En tant que grands producteurs de données de santé, les laboratoires de biologie médicale sont bien entendu en première ligne.

Un délégué à la protection des données. L'une des première obligation est de nommer un Délégué à la protection des données (DPO) au sein du laboratoire. Celui-ci est responsable de la conformité de sa structure avec le règlement. Il doit avant tout cartographier les risques dans le cadre d'une analyse d'impact relative à la protection des données (« Privacy impact assessment » ou PIA). À ce sujet, tous les laboratoires ayant fait leur déclaration de conformité à la Cnil à la NS 53, ils ont trois ans pour faire leur étude impact.

Mettre en place une procédure et une traçabilité écrite. Les laboratoires doivent adopter le concept d'« accountability », à savoir l'obligation de rendre compte. Les LBM, comme tous les autres acteurs de santé concernés, doivent désormais justifier de l'existence et de la fiabilité de leurs procédures relatives à la collecte, l'usage, la protection, le stockage, l'anonymisation ou, encore, à la suppression des données à caractère personnel. Ils doivent également pouvoir démontrer à tout moment qu'ils mettent tout en œuvre, à leur échelle, pour respecter les obligations du règlement. Une démarche que les biologistes connaissent bien puisqu'elle est comparable à celle de l'accréditation.

Respecter les nouveaux droits des patients. Des droits pour les individus sont créés. Parmi eux, notons le « droit à l'effacement » et le « droit à la correction » des données. Ce dernier droit peut avoir des conséquences importantes en matière de ressources pour le laboratoire. Il prévoit le droit pour les personnes d'être informées *« de façon compréhensible et aisément accessible »* sur l'utilisation de leurs données, et de l'être également en cas de violation de leurs données.

Que faire en urgence ?

On l'aura compris : l'objectif est de prendre à bras le corps le problème des données personnelles aujourd'hui produites et traitées par de très nombreux acteurs. De lourdes sanctions sont prévues en cas de manquement et la Cnil a prévenu qu'elle fera bel et bien des contrôles.

Alors, que faire si vous ne vous êtes préoccupé du sujet que tout dernièrement ? Dans l'urgence, il vous est demandé d'être entrée dans la démarche en ayant, au moins : désigné un DPO, établi une cartographie des traitements de données personnelles, rédigé le registre de traitement et commencé à mettre le tout par écrit. ■

1. Règlement européen 2016/679 du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
2. La Cnil a élaboré un guide méthodologique d'aide à la cartographie des risques, disponible en ligne : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-fr-methode.pdf.